

An Example for Use of Public Key

-인증서요청과발급

X.509 인증서 구조

Version

Serial number

Signature algorithm identifier

Issuer name

Period of validity(시작일, 만료일)

Subject name

Subject's public-key information

Issuer unique identifier(Optional)

Subject unique identifier(Optional)

Extensions

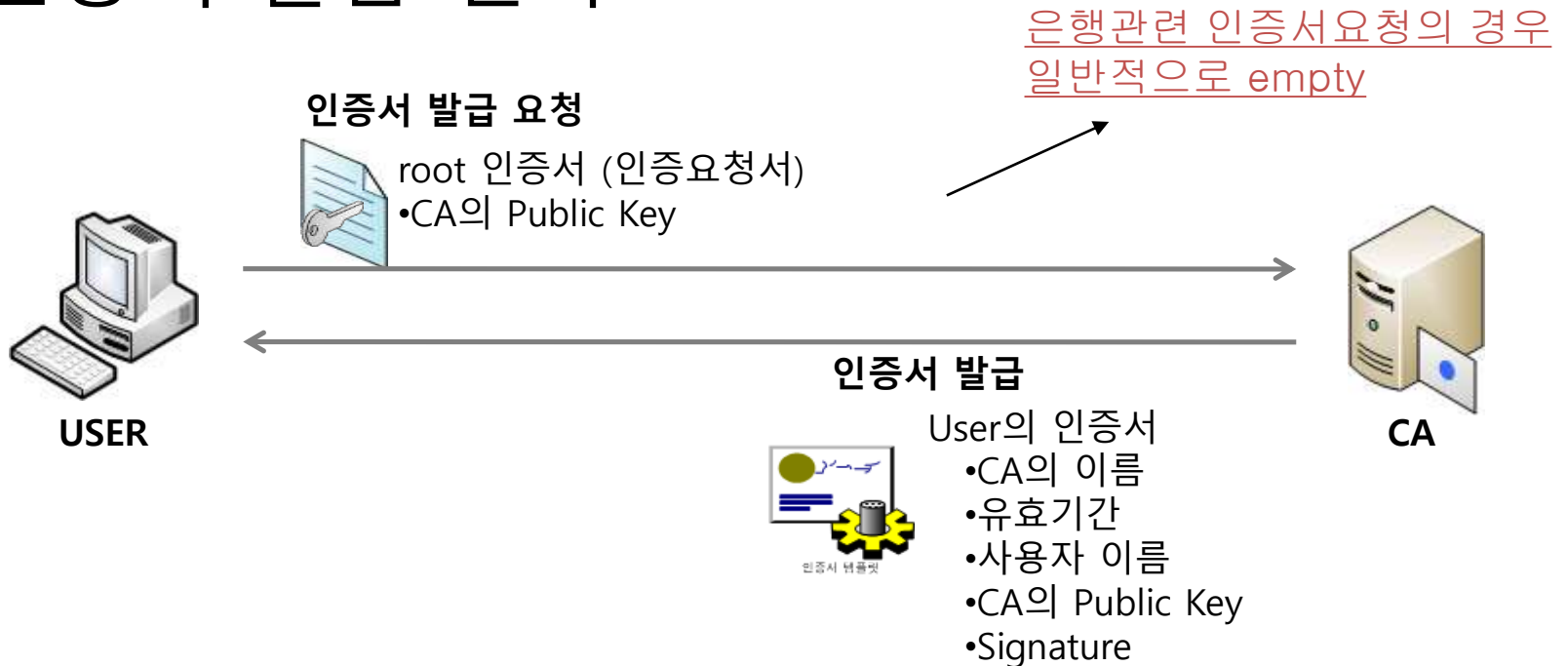
Signature

- Signature algorithm identifier
 - 사용한 해쉬 알고리즘
 - 매개변수
- Subject's public-key information
 - 사용한 공개키 알고리즘
 - 매개변수
 - 공개키
- Signature : 다른 필드 전체로 digest를 만들고, CA의 Private Key로 암호화한다

An Example for Use of Public Key

- 인증서요청과발급

• 인증서 발급 절차

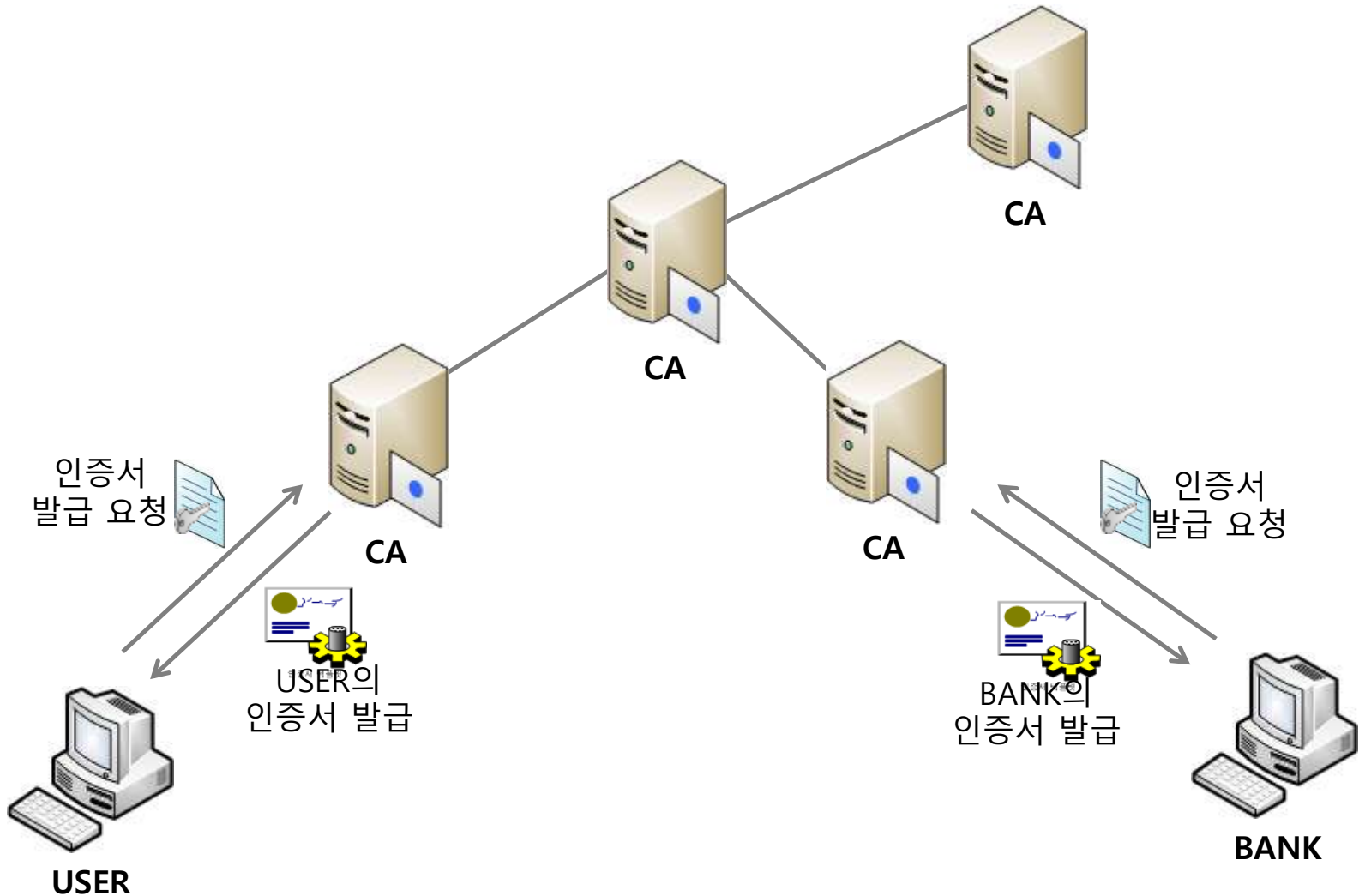


• 인증서의 Signature

Signature를 제외한 모든 필드로 digest를 만들고, 이 digest를 CA의 Private Key로 암호화한 것이다. 일종의 전자서명으로 인증서의 내용이 사실임을 CA가 공증하는 것이다.

An Example for Use of Public Key

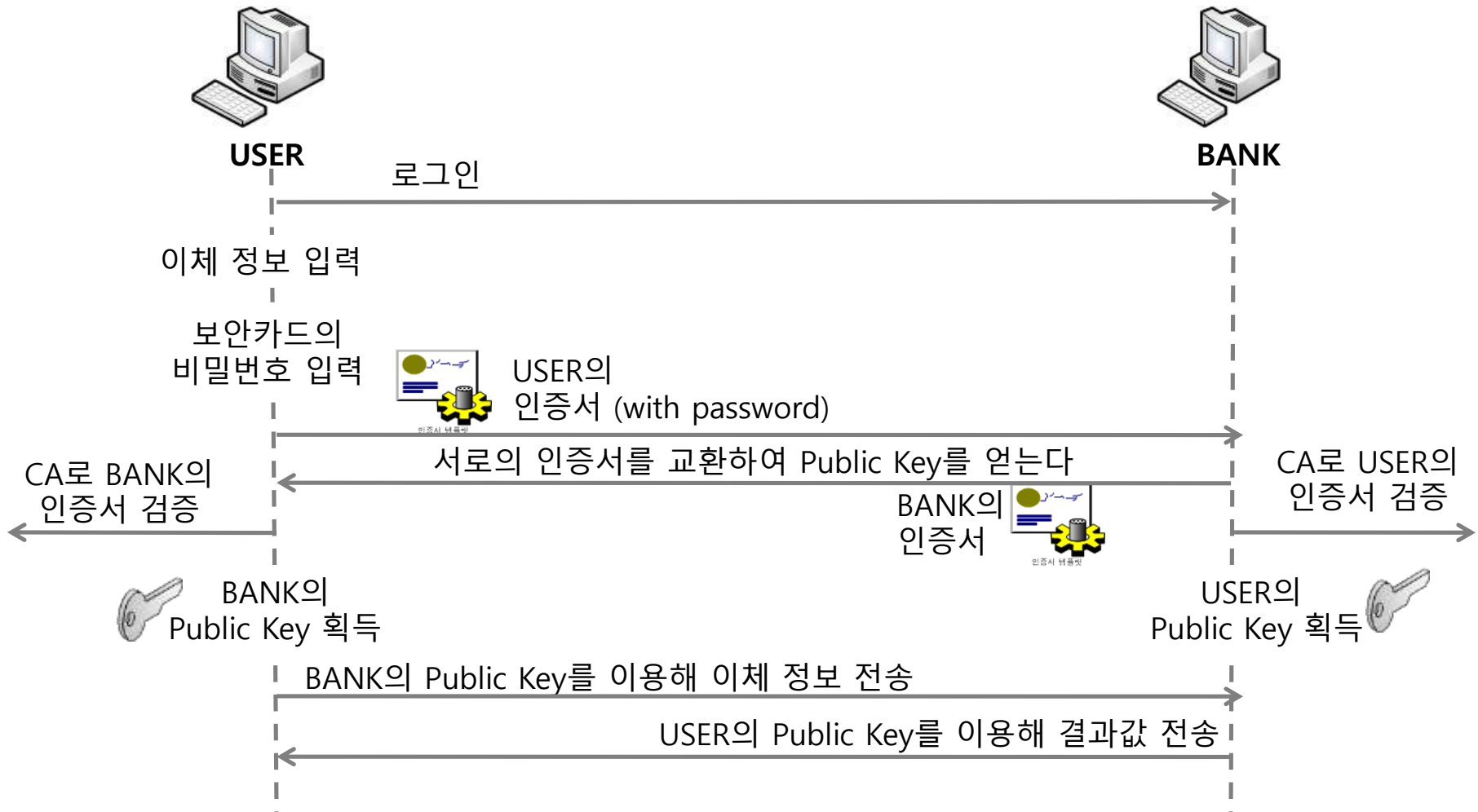
- 인증서요청과 발급



An Example for Use of Public Key

-인증서요청과발급

- 실 예제: 인터넷 뱅킹

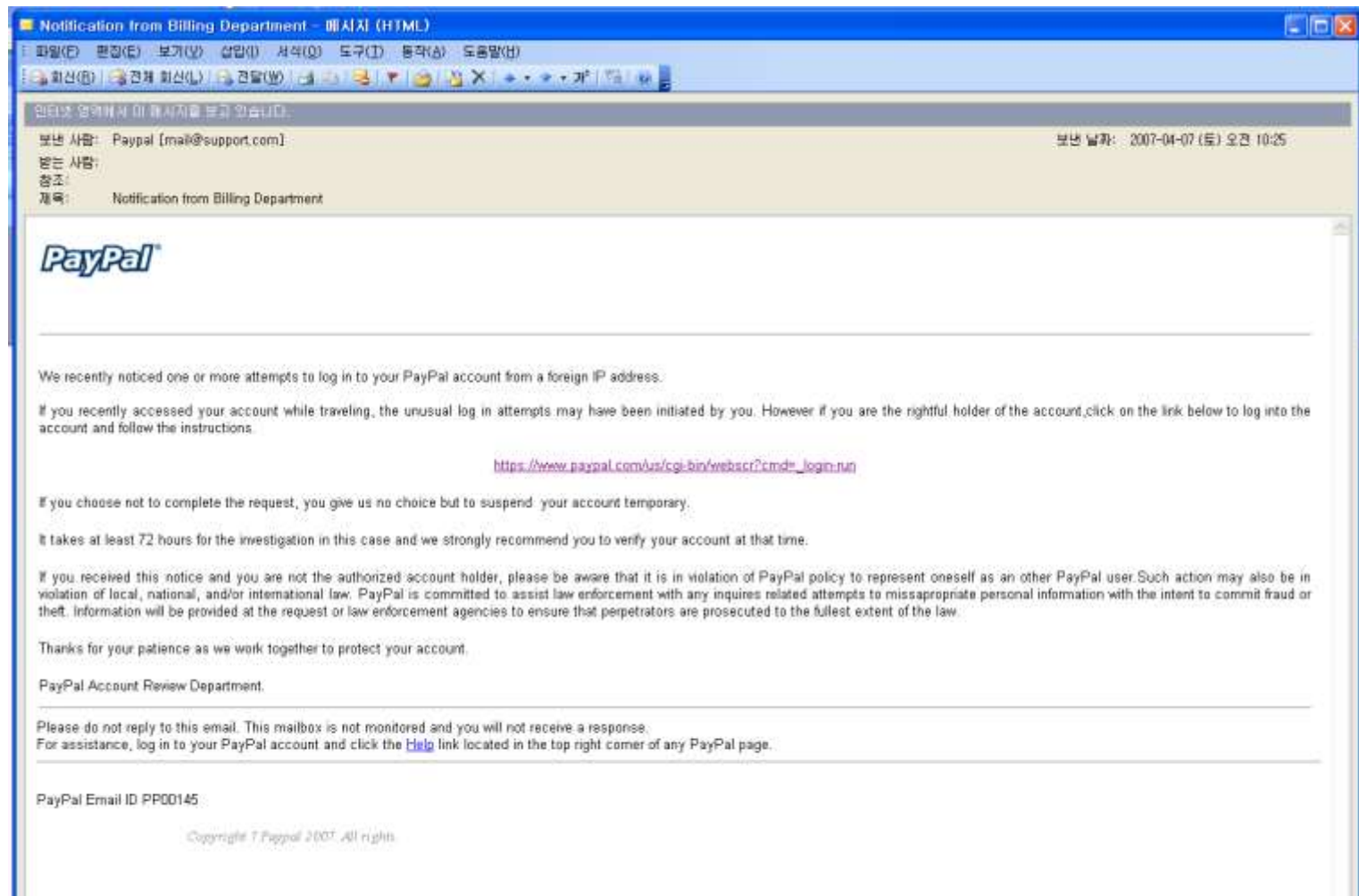


About Phishing

- **Phishing** is a [criminal](#) activity using [social engineering](#) techniques.
- Phishers attempt to [fraudulently](#) acquire sensitive information, such as usernames, [passwords](#) and [credit card](#) details, by masquerading as a trustworthy entity in an electronic communication.
- [Ebay](#) and [PayPal](#) are two of the most targeted companies, and online banks are also common targets.
- Phishing is typically carried out using [email](#) or an [instant message](#), and often directs users to a website, although phone contact has been used as well.

Private data + fishing = Phishing (?)

An Example of Phishing (1)



An Example of Phishing(2)

The image shows a screenshot of a Microsoft Internet Explorer browser displaying a phishing website that mimics the PayPal homepage. The browser's address bar shows a URL: <http://www.futurestem.ru/images/www.paypal.com/cgi-bin/webstrcmd?-login-nur/update.php>. The page features the PayPal logo and navigation links such as "Sign Up", "Log In", "Help", and "Security Center". A main navigation bar includes "Welcome", "Send Money", "Request Money", "Merchant Tools", and "Auction Tools".

The central content area is divided into several sections:

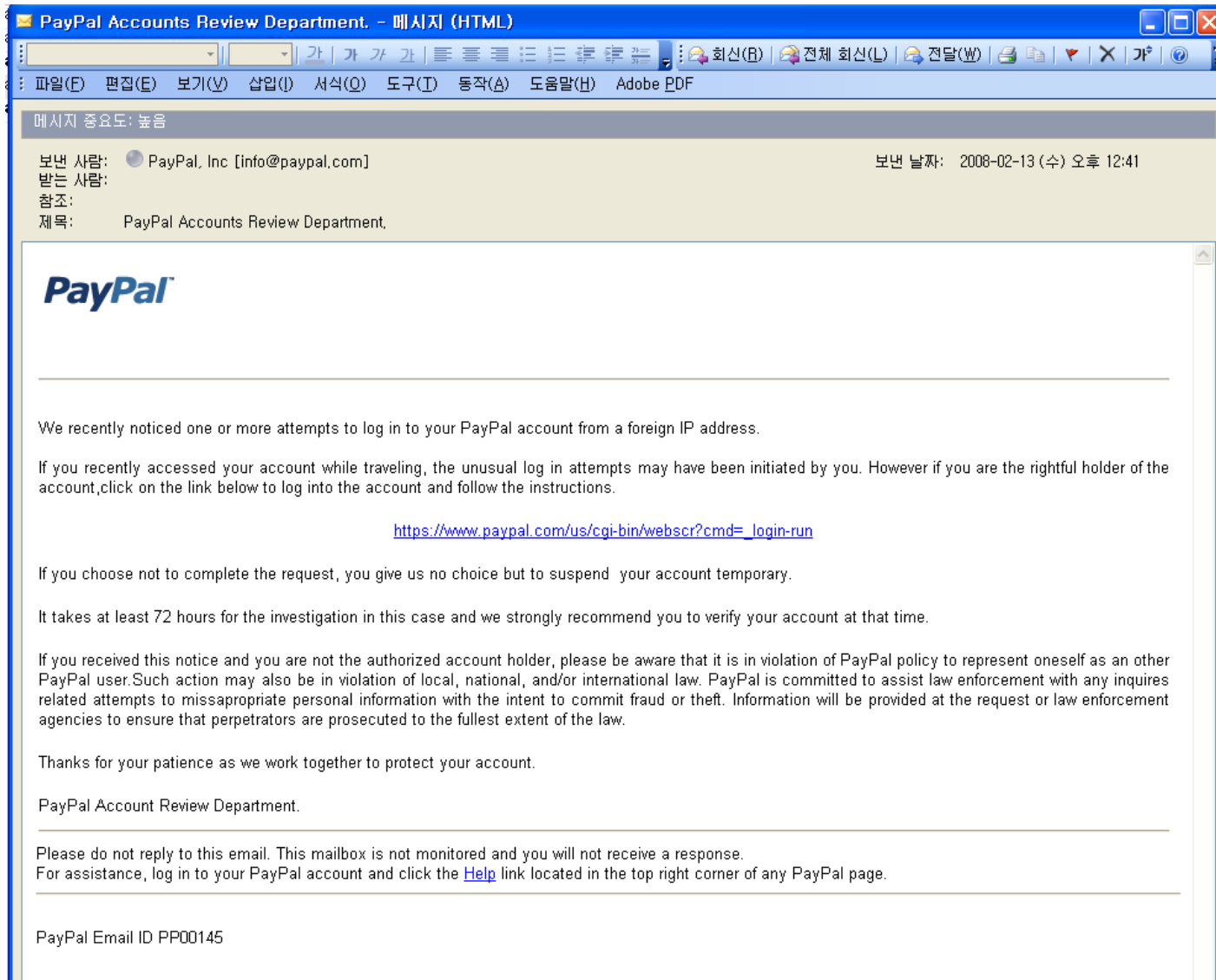
- Member Log-In:** Includes a "Forgot your email address?" link, a "Forgot your password?" link, and input fields for "Email Address" and "Password" with a "Login" button.
- Join PayPal Today:** Promotes "Now Over 100 million accounts" and includes a "Sign Up Now!" button.
- Shop Without Sharing:** A banner with the text "Your Financial Information" and "PayPal. Privacy is built in." with a "Learn more" link.
- Send money NOT your financial info:** A yellow box with a "Watch how PayPal works" link.
- PayPal Mobile:** A section with a "Learn more" link.

Below these sections are three columns of promotional text:

- Buyers:** "Send money with an email address in 103 countries and regions." "PayPal is free for buyers." "Shop without sharing financial information." "100% protection against unauthorized payments sent from your account."
- eBay Sellers:** "Free eBay tools make selling easier." "PayPal works hard to help protect sellers." "PayPal simplifies shopping and tracking." "Earn cash back with PayPal Preferred Rewards."
- Merchants:** "Accept credit cards online with PayPal." "Get paid by phone, fax, and mail with Virtual Terminal." "See how PayPal can increase your sales." "Learn more about our secure Merchant Services." "Compare our solutions site by site."

At the bottom of the page, there are links for "About", "Accounts", "Fees", "Privacy", "Security Center", "Contact Us", "Legal Agreements", "Developers", "Jobs", "Mobile", "Plus Card", "External", "Stores", and "Mass Pay". There are also regional links for Australia, Austria, Belgium, Canada, China, France, Germany, Italy, Netherlands, Poland, Spain, Sweden, and Switzerland. A "100% Verified" logo is present, along with a link to "About SSL Certificates". The footer contains the copyright notice: "Copyright © 1999-2007 PayPal. All rights reserved. Information about FDIC pass-through insurance." and logos for "TRUSTe" and "PRIVACY" (VeriSign).

An Example of Phishing(3)



The image shows a screenshot of a web browser window displaying a phishing email. The browser's title bar reads "PayPal Accounts Review Department. - 메시지 (HTML)". The address bar shows a URL starting with "https://www.paypal.com/". The email header indicates it is from "PayPal, Inc [info@paypal.com]" and was received on "2008-02-13 (수) 오후 12:41". The subject line is "PayPal Accounts Review Department,". The body of the email features the PayPal logo and a message stating that there have been attempts to log in from a foreign IP address. It includes a link to a PayPal login page and a warning that the account will be suspended if the request is not completed. The email concludes with a thank you and the signature "PayPal Account Review Department." and a footer with "PayPal Email ID PP00145".

PayPal Accounts Review Department. - 메시지 (HTML)

메시지 중요도: 높음

보낸 사람: PayPal, Inc [info@paypal.com] 보낸 날짜: 2008-02-13 (수) 오후 12:41
받는 사람:
참조:
제목: PayPal Accounts Review Department.

PayPal

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However if you are the rightful holder of the account, click on the link below to log into the account and follow the instructions.

https://www.paypal.com/us/cgi-bin/webscr?cmd=_login-run

If you choose not to complete the request, you give us no choice but to suspend your account temporary.

It takes at least 72 hours for the investigation in this case and we strongly recommend you to verify your account at that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as an other PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is committed to assist law enforcement with any inquires related attempts to missappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request or law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

PayPal Account Review Department.


Please do not reply to this email. This mailbox is not monitored and you will not receive a response.
For assistance, log in to your PayPal account and click the [Help](#) link located in the top right corner of any PayPal page.

PayPal Email ID PP00145

An Example of Phishing

보낸 사람: Wells Fargo Online <alerts@notify.wellsfargo.com>
받는 사람: iie@khu.ac.kr; cshong@khu.ac.kr; trhahn@khu.ac.kr
참조:
제목: Wells Fargo Checking Account Update

📧 메시지 📎 WellsFargo--CheckingAccount-Status-Report-V94DP-March-2012.zip (48 KB)

wellsfargo.com

An update on your checking account activity

Here is the update you requested for your Wells Fargo checking account XXXXXX3245.

Balance Summary

Ending Balance:	\$11,823.36
Available Balance(as of Tue, 20 Mar 2012 15:56:34 +0100):	\$3,180.54

Deposits

ONLINE TRANSFER REF #IBE4156687 FROM CHECKING XXXXXX7587 ON 01/24/12	\$581.00
---	----------

This information is accurate as of Tue, 20 Mar 2012 15:56:34 +0100. For the most current balance and more account details, open attached report and go to Account Activity Section for this account.

If you have questions, Wells Fargo Online Customer Service is available 24 hours a day, 7 days a week. Call us at 1-800-956-4442 or sign on to send a [secure email](#).

wellsfargo.com | [Fraud Information Center](#)

Note about balances: Ending balance reflects transactions that have posted to your account and does not reflect pending deposits or withdrawals. The available balance is an indication of funds that are available to you today; however, it may not reflect all transactions that you may have initiated or authorized.

Available Balance - This is the amount of money you have in your account that is available for withdrawal. It reflects the latest balance based on transactions posted to your account, including deposited funds, paid checks, withdrawals, and purchases made with your ATM Card or Debit Card. Please note that some transaction activity (such as outstanding checks and some Debit Card purchases) may take several days to post to your account and, therefore, may not be reflected in the available balance. Some deposits made in a store or ATM may not be immediately available for withdrawal or to cover other transactions.

Please do not reply to this email directly. To ensure a prompt and secure response, sign on to email us.

To modify or cancel your alerts, sign on, go to Messages & Alerts, and select Set Up/Modify Alerts.